## Claims

1. A method of using cryptography with biometric verification on security authentication, comprising the steps of:

Utilizing physical immutable identification credentials of a user to perform authentication in conjunction with cryptography technology, and means for providing high security of transmission;

Generating a cryptographic key of the user using the DES algorithm from a user's host;

Encrypting means for using a public key of KDC to encrypt data including said cryptographic key and activated biometric features;

Transmitting means for transmitting said encrypted data from said host to said KDC for decryption; wherein

Decrypting said encrypted data using a private key of KDC to perform verification by collation and comparison; wherein

Collation means for collating said activated biometric features and digitized BIR stored on said KDC;

Comparison means for comparing said decrypted key with the original stored numbers on said KDC;

Approval means for getting approved from said verification, and for releasing the user's private key from said KDC;

Encoding said private key using said cryptographic key for transmitting to say host;

Retrieving said private key from said KDC, and for decoding said private key using said cryptographic key; and

Overcoming the need to carry, store or remember private keys for encryption/decryption.

2. The method of claim 1 wherein said user's host means for comprising a bank card, a credit card, a storage valued card, a magnetic strip card, an IC card, a smart card, an optical card, CD, DVD, a 2D bar code card, portable magnetic storage device, portable electronic memory device and portable mobile storage device.

3. The method of using cryptography with biometric verification on security authentication as defined in claim 1, and further comprising:

Storing said private key of the user in a computer chip; and

Performing the BIR process and encryption/decryption processes of the user by the processor, which relates to calculation, collation and verification as a secured mechanism in the host.

4. The method of claim 3 wherein said computer chip means for comprising RISC CPU, CISC CPU, DSP, FPGA, CPLD, NET ASIC, Microprocessor, Micro controller and other chips with function calculation; and wherein the elements of said chips means for comprising system-on-a-chip (SOC), system-on-multiple-integrated-chips and system-on-multiple-chips.

5. The method of claim 1 wherein said biometric characteristics means for comprising fingerprint, voiceprint, face, iris, retina, palm print, palm shape, signature and other individual biometric characteristics according to the standard of International Biometric Industry Association (IBIA).